Amendments to the Specification:

Please replace the paragraph beginning at page 5, line 27 with the following amended paragraph:

The aggregator 14 can also execute a grouping process 200 that efficiently partitions hosts on a network into groups in a way that exposes the logical structure of the network 18. The grouping process 200 assigns nodes 20 to groups and includes a classification process 200a that classifies hosts by groups and a correlation process 200b that correlates groups. Details of the grouping process are discussed in a paper by Godfrey Tan, Massimiliano Poletto, John V. Guttag, M. Frans Kaashoek entitled "Role Classification of Hosts Within Enterprise Networks Based on Connection Patterns" USENIX Annual Technical Conference, General Track 2003: 15-28. Other role grouping techniques are possible.

Please replace the paragraph beginning at page 6, line 8 with the following amended paragraph:

Referring to FIG. 2, collectors 12 are shown disposed to sample or collect information from network devices 15, e.g., switches as shown. The collector devices 12 send the information to the aggregator 14 over the network 18. The collectors 12 in one configuration 15a sample all traffic from a downstream network 19a provided that the traffic traverses the switches 15, whereas in another configuration 15b the collectors 12 sample traffic from downstream network 19b that enters and leaves the switches 15.

Please replace the paragraph beginning at page 7, line 21 with the following amended paragraph:

Referring to FIG. 3, the aggregator 14 is a device (a general depiction of a general purpose computing device is shown) that includes a processor 30 and memory 32 and storage 34. Other implementations such as Application Specific Integrated Circuits are possible. The aggregator 14 includes a process 36 to collect data from collectors 12 and a process 38 to produce a connection table 40. In addition, the aggregator 14 includes anomaly analysis and alert generation ~~event~~ process 39 to detect anomalies and process anomalies into events that are reported to the operator console or cause the system 10 to take action in the network 18.

Anomalies in the connection table can be identified as events including denial of service attacks, unauthorized access attempts, scanning attacks, worm propagation, network failures, addition of new hosts, and so forth.